

REPUBLIQUE DU CAMEROUN

Paix -Travail-Patrie

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

INSTITUT UNIVERSITAIRE DE LA COTE

Institut d'Ingénierie Informatique d'Afrique Centrale

DEPARTEMENT DU CYCLE MASTER CS2I



**DETECTION / PREVENTION AUTOMATIQUE
D'INTRUSIONS A PARTIR DE CAPTEURS DISTRIBUES
DANS UN RESEAU INFORMATIQUE. Cas d'étude : IP-TELRA**

Rédigé et présenté par :
TIOWA NZONTEU

Matricule :
ISTDI15E010728

Sous la Direction de :
Dr TEGUIA Jean Blaise
M. TEKEU Hypolithe
M. HAMENI Christian

Année Académique : 2021-2022

Sommaire

Sommaire	i
Liste des figures	ii
Liste des tableaux	iii
Introduction	1
Etude de l'existant	2
Matériel et méthode.....	9
Résultat :	13
Conclusion.....	13

Liste des figures

Figure 1: Architecture existante IP-TELRA	3
Figure 2: Code couleur des risques [9].....	8
Figure 3: Solution de sécurisation d'un système informatique.....	9
Figure 4 : Localisation typique d'un capteur et du système Bro.....	13

Liste des tableaux

Tableau 1: Moyen matériel d'IP-TELRA	3
Tableau 2: Moyen logiciel IP-TELRA	4
Tableau 3: Point faible du système existant	6

Introduction

Les réseaux informatiques sont devenus des ressources vitales et déterministes pour le bon fonctionnement des entreprises. De plus, ces réseaux sont ouverts de fait qu'ils sont pour la plus parts raccordés à l'Internet [1]. Cette ouverture qui permet de faciliter la communication, engendre malheureusement des risques importants dans le domaine de la sécurité informatique. Des données récemment publiées par l'Agence nationale des TIC (ANTIC) révèlent des pertes financières de plus de 12 milliards de FCFA au Cameroun dues à la cybercriminalité en 2021, soit deux fois plus que l'année 2019 [2]. Les utilisateurs de l'Internet ne sont pas forcements pleins de bonnes intentions, ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour réaliser leurs attaques. Les conséquences de ces attaques peuvent être lourdes pour un particulier (pertes d'informations, ou pire encore vol d'informations, atteinte à la vie privée...) et pour une entreprise (perte du savoir-faire, atteinte à l'image de marque, perte financière...). Pour cela, les administrateurs déploient des solutions de sécurité efficace capable de protéger le réseau de l'entreprise.

Réduire ou éliminer les failles de sécurité d'un réseau afin de diminuer les risques de concrétisation de menaces est devenu un point important dans la mise en place des réseaux. Parmi les préceptes connus dans le domaine de la sécurité informatique, se trouve celui énonçant que pour une entreprise connectée à l'Internet, le problème aujourd'hui n'est plus de savoir si elle va se faire attaquer, mais quand cela va arriver [3]; une solution possible est alors d'essayer de repousser les risques dans le temps par la mise en œuvre de divers moyens destinés à augmenter le niveau de sécurité du réseau. Il est ainsi nécessaire de disposer d'outils spécialisés dont le rôle sera de surveiller les données qui transitent sur un système et de réagir si certaines semblent suspectes. Les logiciels qui sont les plus à même d'effectuer cette tâche sont les systèmes de détection et de prévention d'intrusions. A notre arrivé au sein de l'entreprise IP-TELRA ce type de système n'existait pas, mettant ainsi l'entreprise dans un état de vulnérabilité permanente face aux attaques bien que celle-ci dispose d'un niveau de sécurité minimale mais ne garantissant pas au mieux la sécurité des données et des entités de son réseau interne en vue de l'importance et de la criticité de celles-ci. Heureusement jusqu'ici nous n'avons pas encore connu le pire au sein d'IP-TELRA mais pour une entreprise en pleine croissance comme tel et dans la mesure d'une sécurité préventive plus accentué car nous comptons dans les statistiques Camerounais plus de 12000 attaques des entreprises entre 2013

et 2017 qui ne cesse d'augmenter d'année en année [2] [4]. L'objectif principal qui nous guide dans ce travail est de proposer une architecture distribuée de détection et de prévention d'intrusions basée sur l'utilisation de systèmes de détection d'intrusions. Nous proposons également un réseau de pots de miel dont le but est d'étudier les menaces contre IP-TELRA, afin de chaque fois réadapter la politique implémentée dans les systèmes de détection contre les nouvelles tendances de menaces. Pour arriver à bien dans notre travail nous devons, Installer Bro IDS pour le filtrage des paquets, Créer des règles de filtrage pour sécuriser de réseau, Installer un ordinateur pot de miel pour tromper les attaquants, Faire communiquer les différents équipements dans le réseau, Mettre en place un réseau d'IDS distribué. Nous proposons dans ce projet, une approche d'architecture distribuée de détection et de prévention d'intrusions basée sur l'utilisation de système de détection d'intrusions. Également, nous proposons un espace d'étude des mécanismes d'attaque, basé sur les pots de miel. La combinaison de ces deux moyens permettra d'offrir un environnement de surveillance un peu plus fiable au réseau de l'entreprise IP-TELRA.

Etude de l'existant

L'analyse de l'existant permet de comprendre la nature du système actuel, décrit la solution présente du domaine d'étude au terme d'organisation. Le but de l'analyse de l'existant est la recherche des points forts et des points faibles du système existant. Ainsi, l'analyse de l'existant fait l'état de lieux du système actuel.

Présentation de l'architecture réseau existante

L'architecture réseau existant à ce jour à IP-TELRA se présente comme suit :

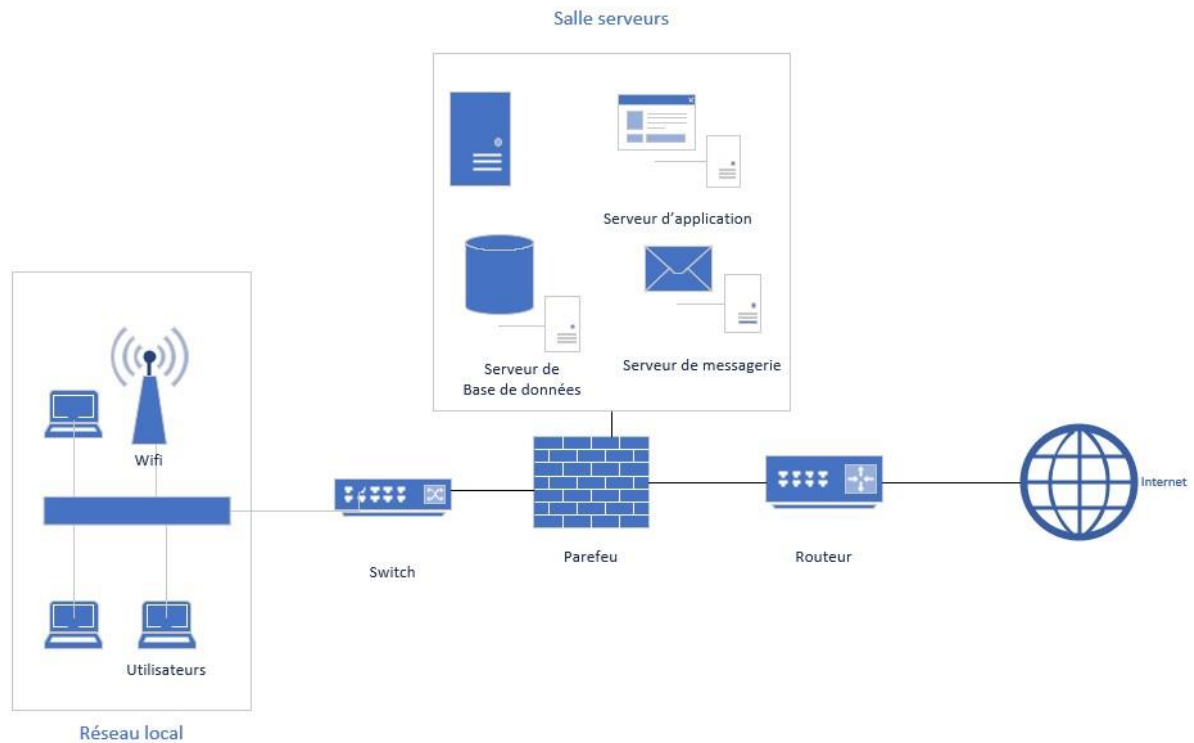


Figure 1: Architecture existante IP-TELRA

Etude des moyens de traitement des informations

Moyens matériels

L'entreprise dispose en son sein d'un grand nombre d'ordinateur, un serveur dédié, des imprimantes, des onduleurs, des stabilisateurs et d'outils disponible pour le réseau (Switch, routeur). Les principaux outils informatiques de la structure sont listés dans le tableau suivant :

Tableau 1: Moyen matériel d'IP-TELRA

Equipements	Nombre	Model	Usage
Routeur	01	Cisco 1921	Gérer le réseau et les connexions
Modem internet	01	Modem Camtel Huawei Hg8245	Accès à internet
Pare-feu	01	Cisco ASA 5505	Contrôle le trafic réseau entrant et sortant
Serveur	04	Serveur tour DELL PowerEdge T430	Stockage des données et des services

Switch	02	Cisco Catalyst 2960	Filtrage et connectivité des postes
Ordinateur fixe	08	DELL Optiplex 790 core i5 8Go ram	Permet aux employé d'effectuer leurs travaux en interne
Ordinateur portable	06	Dell E5450 i5-5300U -8Go ram	Permet aux employé d'effectuer leurs travaux en déplacement
Point d'accès wifi	03	TP-Link TL-WR740N	Donner un accès wifi au utilisateurs
Photocopieur	01	Canon IR Advance C5535i	Permet d'effectuer les taches d'impression et de photocopie

Moyens logiciels

L'entreprise dispose également d'un ensemble de moyen logiciel dans l'accomplissement de ces fonctions. Les logiciels principalement utilisés au sein de la structure sont listés dans le tableau ci-après :

Tableau 2: Moyen logiciel IP-TELRA

Logiciels	Version	Utilité
Logiciels Système		
Windows 10	10 21H2 Professionnelle (Octobre 2021)	Système d'exploitation pour les postes utilisateur
Ubuntu	20.04 23 avril 2020	Système serveur pour les sauvegardes et les répliques
Windows server 2016	1607 (10.0.14393.2363) (10 juillet 2018)	Pour la gestion des postes utilisations, les configurations et prise en charge de certains services et ressources.
Logiciels Applicative		
Microsoft office 2019	2206 (16.0.15330.20246) / 12 Juillet, 2022	Pour les éventuelles saisies, traitement de texte, tableur, note, etc.
Microsoft 365	Version 2208 (Build 15601.20148)	Pour les éventuelles saisies, traitement de texte, tableur, note, etc.

SQL Server 2012	11.0.2100.60 23/04/2021	Pour la gestion de base de données
VS Code	2019 v16.11.6	Pour la conception des sites et des applications
Teams Windows	12.0 (7/28/2021) 6sept. 2022	Pour les réunions en ligne et les échanges
Android-studio-2020	2021.2.1 (Chipmunk) / 9 Mai 2022	Pour la conception des applications Android
Antivirus Kaspersky Total Security	21.3. 10.391 18 juil. 2022	Pour la protection des postes contre les virus informatique
HTML, CSS, JavaScript, JAVA, LARAVEL, C++	/	Comme langage de programmation.

Moyens humains

Le service informatique de la direction générale du Groupe IP-TELRA est composé d'un informaticien qualifié, apte et dynamique capable d'assumer avec tant de dévouement les missions qui lui est assignées.

Le but du critique de l'existant est de recenser les points forts et faibles du système en cours ; Dans ce cas, l'analyste procède à une critique objective du système en cours.

Les points fort du système existant

Dans cette section nous soulevons les points forts dans l'organisation, l'architecture et la sécurité de la structure d'IP-TELRA.

Du point de vue moyen humain : La direction générale du Groupe IP-TELRA regorge en son sein un personnel qualifié et dynamique pour assurer la plupart de ces fonctions ;

Du point du système d'information : Il est utile de préciser que cela est encourageant de constater qu'au sein de la direction générale du Groupe IP-TELRA, les postes de travail sont opérationnels et occupés par un personnel apte à effectuer le travail au poste auquel il est affecté.

Du point de vue technique : nous notons la présence d'un serveur de réplication et de sauvegarde afin de garantir la disponibilité des données en cas de sinistre ainsi qu'un système de continuité d'énergie en cas de panne électrique.

Du point de vue maintenance : l'équipe de maintenance système assure les mises à jour régulières et correctives en termes de sécurité pour la totalité des systèmes d'exploitation et logiciels.

Du point de vue contrôle d'accès : l'administrateur adapte la politique de blocage de lecteur USB et le filtrage d'accès depuis et vers le réseau internet pour éviter le risque de propagation des virus.

Du point de vue sécurité : Chaque poste de travail dispose d'un antivirus Kaspersky à jour. L'architecture est protégée par un pare feu physique Cisco situé à l'entrée du réseau, il filtre le trafic venant de l'extérieur du réseau afin de détecter d'éventuelles menaces.

Les points faibles du système existant

Dans cette section nous soulevons les manquements à la sécurité dans l'architecture, les solutions et la politique de sécurité d'IP-TELRA.

Le premier manquement à la sécurité ici et qui présente un intérêt particulier pour nous est l'absence d'un système de sécurité robuste pour faire face aux éventuelles attaques des pirates informatique. Ils se limite ici juste à une sécurité assez minimale et basique qui est largement insuffisant quant' à l'importance des données à sécuriser.

Nous notons par ailleurs d'autres manquement à la sécurité répertorié ici par degré de criticité croissant à savoir :

Tableau 3: Point faible du système existant

Danger	Risque	Seuil de criticité
--------	--------	--------------------

La lenteur dans la transmission des données au sein de la hiérarchie de l'entreprise.	Lenteur dans les transmissions et les prises de décision en cas de sinistre.	
Absence d'un guide de procédure.	Mauvaise reprise des activités en cas de sinistre. Lenteur dans l'exécution des tâches.	
Absence d'une politique de sécurité.	Menace non détectée, pas d'évaluation de risques et pas de plan de reprise d'activité.	
Audit de sécurité non effectué au sein de la structure depuis sa création	Détermination des points faibles afin de pouvoir y remédier, non respects des normes	
L'insuffisance des informaticiens pour les multiples tâches qui y sont effectuées.	Surcharge dans le travail qui conduit à la baisse de la productivité.	
Absence d'une politique sur le renforcement des mots de passe.	Vol de mots de passe, usurpation d'identité, vol d'informations	
L'absence d'un système de monitoring.	Interruption d'activité par suite d'une défaillance du matériel ou du logiciel	
L'absence d'un système de détection d'intrusion dans le réseau et d'un moyen d'anticiper sur les menaces liées à l'accès des données via internet.	Attaques de pirate informatique, pertes d'information et de données sensibles, pertes financières.	
L'absence d'une équipe dédiée à la veille, au monitoring de la sécurité et à l'investigation sur les incidents de sécurité.	Piratage du réseau, intrusions d'un agent malveillant au réseau, pertes d'informations et pertes financières.	

Description	Code de couleur
Danger immédiat	
Risque élevé	
Risque moyen	
Faible risque	
Très faible risque	

Figure 2: Code couleur des risques [9]

Quelques propositions de solution

En réponse à l'ensemble des menaces observé au sein de la structure, nous proposons un ensemble de solution [8]















<input type="checkbox"/>  <p>Évaluation de sécurité</p> <p>Il est important d'établir une base de référence et de corriger les vulnérabilités existantes. À quand remonte votre dernière évaluation?</p>	<input type="checkbox"/>  <p>Hameçonnage</p> <p>Sécurisez votre messagerie. 90% des violations de sécurité commencent par ce type d'attaque. Et ce type de courriel devient de plus en plus difficile à repérer. Nous vous aiderons à former votre personnel et à fournir des solutions pour protéger votre entreprise et votre personnel contre ces attaques.</p>	<input type="checkbox"/>  <p>Mots de passe</p> <p>Appliquez des politiques de sécurité sur votre réseau. Vous devriez, par exemple, refuser ou limiter l'accès au stockage de fichiers USB, activer des stratégies de mot de passe améliorées, définir les délais d'expiration de l'écran des utilisateurs et limiter l'accès des utilisateurs.</p>
<input type="checkbox"/>  <p>Sensibilisation à la sécurité</p> <p>Formez vos utilisateurs - souvent! Sensibilisez les à la sécurité des données, aux attaques par courriel et à vos politiques et procédures. Nous proposons une solution de formation en ligne et des politiques de sécurité « faites pour vous ».</p>	<div> <div>Le Saviez-Vous?</div> <div> <div>1 PME sur 5</div> <div>81%</div> <div>97%</div> </div> <div> <div>sera victime d'une cyber-brèche cette année</div> <div>de toutes les violations concernent des PME.</div> <div>des violations auraient pu être évitées grâce à la technologie actuelle.</div> </div> </div>	<input type="checkbox"/>  <p>Détection et réponse avancées</p> <p>Protégez les données de votre ordinateur contre les logiciels malveillants, les virus et les cyberattaques grâce à une sécurité avancée des points d'extrémité. La dernière technologie actuelle (qui remplace votre solution antivirus obsolète) protège contre les menaces sans fichier et celles basées sur des scripts, et peut même annuler une attaque par ransomware.</p>
<input type="checkbox"/>  <p>Authentification multifacteur</p> <p>Utilisez l'authentification multifacteur chaque fois que vous le pouvez, y compris sur votre réseau, les sites Web bancaires et même les médias sociaux. Il ajoute une couche de protection supplémentaire pour garantir que même si votre mot de passe est volé, vos données restent protégées.</p>	<input type="checkbox"/>  <p>Mises à jour des logiciels</p> <p>Mettez à jour les produits tels ceux de Microsoft, Adobe et Java pour une meilleure sécurité. Nous fournissons un service de « mise à jour critique » via l'automatisation pour protéger vos ordinateurs des dernières attaques connues.</p>	<input type="checkbox"/>  <p>Recherche sur le web clandestin</p> <p>Savoir en temps réel quels mots de passe et comptes ont été publiés sur le Dark Web vous permettra d'être proactif dans la prévention d'une violation de données. Nous analysons le Dark Web et prenons des mesures pour protéger votre entreprise contre les informations d'identification volées qui ont été mises en vente.</p>
<input type="checkbox"/>  <p>Gestion des incidents et événements de sécurité (SIEM)</p> <p>Utilisez l'analyse de données pour examiner tous les journaux d'événements et de sécurité de tous les appareils couverts afin de se protéger contre les menaces avancées et de répondre aux exigences de conformité.</p>	<input type="checkbox"/>  <p>Sécurité de la passerelle Web</p> <p>La sécurité Internet est une course contre la montre. La passerelle détecte les menaces et les infections de sécurité web et courriel à mesure qu'elles apparaissent sur Internet, et les bloque sur votre réseau en quelques secondes, avant qu'elles n'atteignent l'utilisateur.</p>	<input type="checkbox"/>  <p>Sécurité des appareils mobiles</p> <p>Les cybercriminels d'aujourd'hui tentent de voler des données ou d'accéder à votre réseau via les téléphones et tablettes de vos employés. Ils comptent sur vous pour négliger cette pièce du casse-tête. La sécurité des appareils mobiles comble cette lacune.</p>
<input type="checkbox"/>  <p>Pare-feu</p> <p>Activez les fonctionnalités de détection et de prévention des intrusions. Envoyez les fichiers journaux à un SIEM géré. Pour plus d'information, appelez-nous dès aujourd'hui!</p>	<input type="checkbox"/>  <p>Chiffrement</p> <p>Dans la mesure du possible, l'objectif est de chiffrer les fichiers au repos, en mouvement (pensez aux courriels) et, ce, surtout sur les appareils mobiles.</p>	<input type="checkbox"/>  <p>Sauvegarde</p> <p>Sauvegarde locale. Sauvegarde dans le cloud. Ayez une sauvegarde hors ligne pour chaque mois de l'année. Testez souvent vos sauvegardes. Et si vous n'êtes pas convaincu que vos sauvegardes fonctionnent correctement, appelez-nous dès que possible.</p>

Figure 3: Solution de sécurisation d'un système informatique

Matériel et méthode

L'analyse fonctionnelle d'un projet informatique est une étape qui s'avère nécessaire et primordial pour mener à bien ce dernier. Elle permet de concevoir un système pour lequel toutes les options seront parfaitement conçues, orientées vers une satisfaction client maximale. C'est dans cette optique qu'avant de commencer ce projet, nous analyserons de manière exhaustive son environnement afin de comprendre les enjeux et les contraintes potentielles.

Présentation du projet

Avec l'évolution des techniques de communication, les systèmes d'information et réseaux informatiques sont aujourd'hui de plus en plus ouverts sur le monde extérieur notamment avec Internet. Cette ouverture facilite la vie pour l'humain en lui offrant divers services, et relie des centaines de millions de machines à Internet un peu partout dans le monde. Cependant, cette interconnexion des machines permet également aux utilisateurs malveillants d'utiliser ces ressources et profiter de ses vulnérabilités à des fins abusives, par exemple : rendre un service web hors ligne.

La sécurité de nos jours est un problème d'une importance capitale, elle est devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers. Différents mécanismes ont été mis en place pour faire face à ces problèmes de sécurité, comme les antivirus, les pare-feux, le cryptage, mais ces mécanismes ont des limites face au développement rapide des techniques de piratage. Pour éviter ces limites, l'utilisation des systèmes de détection d'intrusion s'impose.

Les systèmes de détection d'intrusions ont été conçus pour une surveillance continue, et la découverte des violations de la politique de sécurité, ainsi l'identification de toute activité non autorisée dans un réseau. Les pots de miel quant' à eux sont utilisés pour tromper les pirates afin de recueillir les informations sur les modes d'actions dans le réseau. Le système distribué permet le partage des informations sur les attaques en temps réels dans les différents sites afin que les mesures soient prises pour contrer cela.

Problématique

IP-TELRA étant une jeune entreprise offrant des services par ailleurs les services de stockage en ligne chez certains de ces partenaires, il comporte un grand nombre de données pour la plupart confidentielle dont le piratage pourrait s'avérer fatale pour l'entreprise. Jusqu'à là, aucune étude n'a encore été menée en vue de garantir aux administrateurs de savoir exactement les types de données (offensifs ou non) qui transitent sur les installations du réseau ainsi que les types d'activités exécutées par les utilisateurs qui y sont connectés. Il ne faudrait pas toujours attendre que le drame ne se produit avant de prendre des mesures correctives. La sécurité se doit d'être préventive au maximum afin de pouvoir éviter les éventuelles menaces. Le risque de zéro n'existant pas en matière de sécurité, nous pouvons tout de même s'y rapprocher en mettant en place un bon système de sécurité. Il est donc nécessaire de proposer au réseau un environnement de contrôle des types d'activités (offensif ou non) qui s'y opèrent. Aussi, est-il important de disposer d'un espace d'étude des attaques qui viseraient les équipements du réseau. Cela permettra aux administrateurs du réseau de suivre les nouvelles failles exploitées par les pirates ainsi que les nouveaux outils d'hacking.

Méthodologie et choix techniques

Notre proposition nécessite l'utilisation de plusieurs outils notamment les systèmes de détection d'intrusions (IDS) et les pots de miel. Nous présentons ici notre méthodologie de travail et les choix techniques opérés.

Méthodologie de travail

Ce travail se focalise sur les réseaux de grande étendue de façon générale et IP-TELRA en particulier. Dans ce réseau, nous distinguons les réseaux clients d'IP-TELRA et les infrastructures privées (serveurs de services et équipements réseaux) du réseau lui-même. Ainsi, il est nécessaire de procéder à l'analyse des données sur chaque site du réseau. Pour cela, nous étudions les systèmes de détection d'intrusions en vue de choisir le système le plus approprié selon nos objectifs notamment la communication entre instances autonomes. Ce choix nous permet de former notre environnement distribué sur tout le réseau. Ensuite, nous proposons l'espace d'étude des stratégies, des outils et des commandes utilisés par les pirates, en vue de

chaque fois adapter la politique de sécurité de tout le réseau aux nouvelles tendances de menaces. Il s'agit précisément d'un réseau de pots de miel. Nous analysons donc les types de pots de miel ainsi que les technologies de déploiement de honeynet (réseau de pots de miel) dans le but d'offrir le meilleur environnement possible. L'étape finale est consacrée aux différents tests afin de valider nos différentes propositions.

Choix du système de détection d'intrusion

Il existe différents systèmes de détection d'intrusions avec différentes caractéristiques que nous avons étudiés au chapitre 3. Pour la surveillance de chaque site client d'IP-TELRA, nous utilisons un système de détection d'intrusions réseau. Les IDS réseau sont plus appropriés en ce sens qu'ils ne nécessitent non seulement pas de toucher les machines déjà en production mais aussi permettent de surveiller tout un ensemble de machines à partir d'un point unique. C'est donc une technologie moindre coût nécessitant moins de ressources. De plus, ils ne surchargent pas le réseau et permettent une gestion plus facile de la maintenance. Dans la littérature, les outils les plus évolués pouvant permettre de réaliser cette fonction sont Snort, Suricata et Bro. Notre approche se base sur une architecture distribuée avec des agents complètement autonomes. Dans cette architecture, nous établissons des communications entre les différents agents. Donc, le NIDS doit nous permettre d'implémenter cela. Ainsi, Bro s'est révélé comme l'outil de choix. Comparativement à ces concurrents direct, Bro est nettement une technologie plus avancée. Il donne la possibilité de le personnaliser selon les objectifs désirés. Il est flexible avec un langage incorporé pouvant permettre de créer toute sorte d'outils réseau.

Taches effectuées par Bro (Zeek)

Zeek effectue deux tâches clés qui profitent aux organisations de sécurité :

- 1) Convertit les données sur le trafic réseau en événements de niveau supérieur ;
- 2) Fournit un interpréteur de script, un langage de programmation robuste qui est utilisé pour interagir avec les événements et comprendre ce que ces événements signifient en termes de sécurité du réseau.

En d'autres termes, Zeek capture des métadonnées sur l'activité sur un réseau, puis fournit un langage de programmation pour comprendre quand cette activité présente des indications malveillantes ou suspectes.

Bro par rapport aux IDS conventionnels

Lorsque Bro (Zeek) surveille un flux de trafic, il produit des journaux qui enregistrent tout ce qu'il comprend de l'activité du réseau. Cette compréhension inclut les enregistrements de connexion, le volume de paquets envoyés et reçus, les attributs des sessions TCP et d'autres métadonnées utiles pour analyser le comportement du réseau et comprendre le contexte de ce comportement.

Qu'est-ce qui est considéré comme un comportement réseau suspect dans une organisation, peut-être routinier dans une autre ? C'est pourquoi le langage de programmation Bro (Zeek) est si avantageux ; il peut être utilisé pour personnaliser l'interprétation des métadonnées aux besoins spécifiques d'une organisation.

Bro (Zeek) fournit un moyen d'effectuer les mêmes types de vérifications pour les attributs de trafic, mais avec la valeur ajoutée d'une interface de programmation. Cela signifie que Bro (Zeek) peut être utilisé pour calculer des statistiques numériques et des correspondances de modèles d'expressions régulières. Il peut également créer des conditions logiques complexes à l'aide des opérateurs AND, OR et NOT, qui permettent aux utilisateurs de personnaliser l'analyse en fonction de leur environnement.

Spécification de déploiement de Bro

Le déploiement de Bro dépend fortement de la politique de sécurité adoptée par l'organisation. Placé derrière un pare-feu externe, cette configuration permet à Bro de ne recevoir que des paquets filtrés conformément aux règles définies dans le pare-feu. Cela donne lieu à moins de notifications. Néanmoins certaines organisations préfèrent l'installer sans ce pare-feu dans le but de se voir notifier toutes les tentatives d'attaques. Une autre option est de le placer derrière le pare-feu interne lui permettant de détecter les machines internes infectées par les virus et les vers.

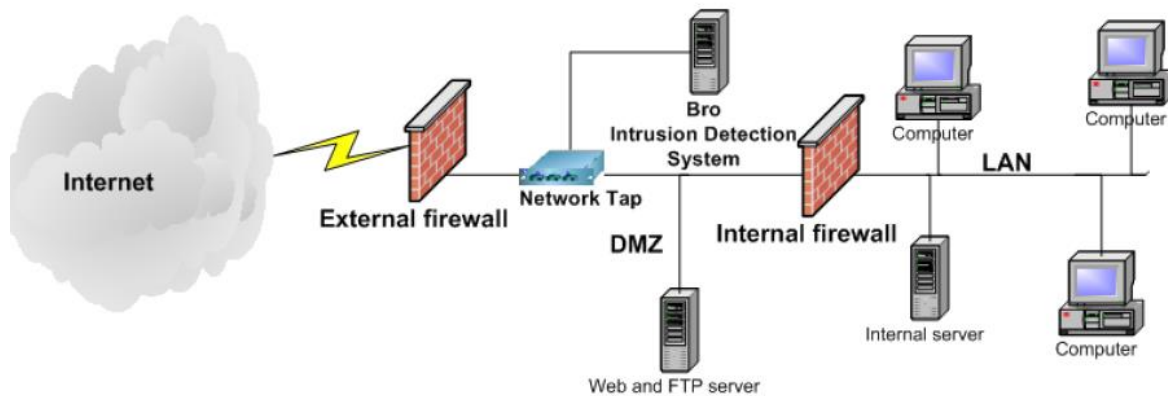


Figure 4 : Localisation typique d'un capteur et du système Bro

Bro ne requiert pas une machine spécialisée, et peut bien fonctionner sur une machine bon marché. Cependant le système doit contrôler tous les paquets entrant et sortant du site. Ainsi suivant le trafic réseau, il peut être nécessaire d'employer une machine assez robuste.

Le tableau suivant donne un récapitulatif des besoins requis pour le déploiement de Bro selon les caractéristiques du réseau de l'hôte.

Résultat :

Nous avons pu mettre en place un système de détection et prévention d'intrusion en utilisant le système de prévention et de détection d'intrusion bro couplé à un réseau pot de miel permettant ainsi de réduire le niveau de vulnérabilité de l'entreprise. Nos principaux défis rencontrés ont été au niveau de la complexité de mise en œuvre et aussi dans l'acquisition du matériel sophistiqué pour pouvoir supporter la solution

Conclusion

La surveillance des données qui transitent sur un réseau permet non seulement de se protéger des menaces, mais aussi d'éviter d'être une zone de transit d'attaques. Dans ce projet, le but de notre travail était de mettre en place un système de détection et de prévention

d'intrusion à l'aide des capteurs distribués dans un réseau à fin d'accroître le niveau de sécurité de l'entreprise IP-TELRA, nous avons proposé de façon générale, une architecture distribuée de détection et de prévention d'intrusions basée sur des agents autonomes ; puis nous l'avons intégré à l'architecture du réseau IP-TELRA. Nous avons dans cette optique utilisé le NIDS Bro que nous avons déployé en tant qu'analyseur réseau sur chaque site. Chaque instance de l'architecture partage des événements avec les autres instances. Pour réaliser cela, nous avons développé en langage Bro deux scripts : `sender.bro` et `receiver.bro`. Ces scripts permettent donc d'établir la communication en les différents agents ainsi que les réactions à adopter lors de l'apparition de ces événements. En outre, nous avons proposé un réseau de pots de miel destiné à l'étude des attaques et outils de piratage. Les informations collectées dans cet espace permettront de suivre les vulnérabilités que les pirates pourraient exploiter dans le réseau IP-TELRA. En conséquence, les administrateurs devront adopter la réaction nécessaire pour réduire ces vulnérabilités.

Afin de pouvoir bénéficier des avantages d'une gestion centralisée, nous proposons comme perspective à ce travail, l'implémentation des mécanismes de collecte d'événements ou d'alertes vers une entité de gestion centrale. Nous aurions alors une architecture provenant d'une combinaison d'architecture distribuée basée sur des agents complètement autonomes et d'architecture distribuée centralisée. Aussi, avec les possibilités offertes par Bro, il serait utile d'instrumenter c'est-à-dire réécrire, à l'aide de Broccoli, les applications (SSH, HTTPS, etc) qui tournent sur les serveurs du honeynet pour qu'elles envoient à Bro, les données qu'elles ont effectivement reçues. Cela permettra par exemple de traquer les connexions cryptées qu'il n'est pas possible d'analyser au niveau réseau.